ISSN 1995-0802, Lobachevskii Journal of Mathematics, 2018, Vol. 39, No. 7, pp. 961–966. © Pleiades Publishing, Ltd., 2018.

Efficient Branching Programs for Quantum Hash Functions Generated by Small-Biased Sets

M. F. Ablayev*

(Submitted by A. M. Elizarov)

Institute of Computational Mathematics and Information Technologies, Kazan (Volga region) Federal University, ul. Kremlevskaya 18, Kazan, Tatarstan, 420008 Russia

Received December 6, 2017

Abstract—In the paper we consider quantum (δ, ϵ)-hash functions in so called phase form (phase quantum (δ, ϵ)-hash function). It is known that ϵ-biased sets generate phase quantum (δ, ϵ)-hash function. We show that the construction is invertible, that is, phase quantum (δ, ϵ)-hash function defines ϵ-biased sets. Next, we present an efficient (in the sense of time and qubits needed) Branching program construction for phase quantum (δ, ϵ)-hash function.

DOI: 10.1134/S199508021807003X

Keywords and phrases: *Quantum computations, Branching programs, Hash function.*

1. INTRODUCTION

Hashing is important tool in Computer Science and Cryptography. In [1] explicitly defined a notion of quantum hashing as a generalization of classical hashing and presented examples of quantum hash functions. Unlike classical hash functions that are secure under some computational assumptions, these functions have "unconditionally one-way" property based on Holevo Theorem [2].

Recall that in the classical setting a cryptographic hash function h should be computed efficiently and should have the following properties (see for example [3]). (1) Pre-image resistance: Given $h(x)$, it should be difficult to find x, that is, these hash functions are one-way functions. (2) Second pre-image resistance: Given x_1, it should be difficult to find an x_2, such that $h(x_1) = h(x_2)$. (3) Collision resistance: It should be difficult to find any pair of distinct x_1, x_2, such that $h(x_1) = h(x_2)$. Note, that there are no classical one-way functions that are known to be provably more difficult to invert than to compute, the security of such cryptographic hash functions is "computationally conditional."

In the paper we consider a quantum hash function construction based on ϵ-biased sets [4]. Such a function $\psi : \mathbb{F}_q \to (\mathcal{H}^2)^{\otimes s}$ hashes elements of finite field $\mathbb{F}_q$ into the s-qubit quantum states. The notion of (δ, ϵ)-hash function combines the notion of pre-image (one-way) quantum δ-resistance property and the notion of quantum collision ϵ-resistance property. These properties are quantum generalizations of classical one-way resistance and collision resistance properties required for classical hash functions. We show that the construction of quantum hash function based on small biased set is reversible.

An important part of the one-way property is computational efficiency. In this paper we show that the considered construction of quantum (δ, ϵ)-hash function can be computed efficiently in the model of Quantum Branching Programs (QBP) [5]. We consider two complexity measures: a number of qubits that a QBP uses for computation and a number of computational steps (or instructions) that QBP performs. Such a QBP for the function $\psi : \mathbb{F}_q \to (\mathcal{H}^2)^{\otimes s}$ requires $s = O(\log \log q)$ qubits and performs $\log q$ steps.

We prove that the proposed QBP construction is optimal. That is, we prove lower bounds of $\Omega(\log \log q)$ for the memory and $\Omega(\log q)$ for the time of quantum (δ, ϵ)-hash function implementation.

*E-mail: mablayev@gmail.com